

WE CLAIM:

1. A computer program product for controlling a computer to scan a compressed
5 computer file for malware, said compressed computer file being compressed using a
compression algorithm, said computer program product comprising:

comparison code operable to compare a plurality of compressed malware
signatures compressed using said compression algorithm with said compressed
computer file to identify malware within said compressed computer file.

10 2. A computer program product as claimed in claim 1, further comprising:
detection code operable to detect from a compressed computer file to be
scanned what compression algorithm has been used to compress said compressed
computer file; and

15 compression code operable to compress a plurality of uncompressed malware
signatures using said detected compression algorithm to generate said plurality of
compressed malware signatures.

20 3. A computer program product as claimed in claim 2, wherein said detection
code reads compression algorithm specifying data from said compressed computer
file.

25 4. A computer program product as claimed in claim 3, wherein said compression
algorithm uses Huffman coding and said compression algorithm specifying data
includes a Huffman coding table used to compressed said compressed computer file.

30 5. A computer program product as claimed in claim 1, wherein said comparison
code uses a Boyer Moore algorithm or an algorithm based upon structuring the
signatures in a tree.

6. A computer program product as claimed in claim 1, wherein said malware
includes at least one of computer viruses, Trojans, worms, banned files and e-mails
containing banned content.

7. A method of scanning a compressed computer file for malware, said compressed computer file being compressed using a compression algorithm, said method comprising the step of:

comparing a plurality of compressed malware signatures compressed using said compression algorithm with said compressed computer file to identify malware within said compressed computer file.

8. A method as claimed in claim 7, further comprising the steps of:

detecting from a compressed computer file to be scanned what compression algorithm has been used to compress said compressed computer file; and
compressing a plurality of uncompressed malware signatures using said detected compression algorithm to generate said plurality of compressed malware signatures.

9. A method as claimed in claim 8, wherein said step of detecting reads compression algorithm specifying data from said compressed computer file.

10. A method as claimed in claim 9, wherein said compression algorithm uses Huffman coding and said compression algorithm specifying data includes a Huffman coding table used to compressed said compressed computer file.

11. A method as claimed in claim 7, wherein said step of comparing uses a Boyer Moore algorithm or an algorithm based upon structuring the signatures in a tree.

12. A method as claimed in claim 7, wherein said malware includes at least one of computer viruses, Trojans, worms, banned files and e-mails containing banned content.

13. Apparatus for scanning a compressed computer file for malware, said compressed computer file being compressed using a compression algorithm, said apparatus comprising:

comparison logic operable to compare a plurality of compressed malware signatures compressed using said compression algorithm with said compressed computer file to identify malware within said compressed computer file.

14. Apparatus as claimed in claim 13, further comprising:

detection logic operable to detect from a compressed computer file to be
scanned what compression algorithm has been used to compress said compressed
5 computer file; and

compression logic operable to compress a plurality of uncompressed malware
signatures using said detected compression algorithm to generate said plurality of
compressed malware signatures.

10 15. Apparatus as claimed in claim 14, wherein said detection logic reads
compression algorithm specifying data from said compressed computer file.

16. Apparatus as claimed in claim 15, wherein said compression algorithm uses
Huffman coding and said compression algorithm specifying data includes a Huffman
15 coding table used to compressed said compressed computer file.

17. Apparatus as claimed in claim 13, wherein said comparison code uses a Boyer
Moore algorithm or an algorithm based upon structuring the signatures in a tree.

20 18. Apparatus as claimed in claim 13, wherein said malware includes at least one
of computer viruses, Trojans, worms, banned files and e-mails containing banned
content.